UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/805,702	03/22/2004	Steven J. Winick	H0006502-0555 (17268)	8726

128 7590 12/18/2007

HONEYWELL INTERNATIONAL INC.
101 COLUMBIA ROAD
P O BOX 2245
MORRISTOWN, NJ 07962-2245

EXAMINER	
YOUNG, NICOLE M	

ART UNIT	PAPER NUMBER
2139	

MAIL DATE	DELIVERY MODE
12/18/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/805,702	WINICK, STEVEN J.	
	Examiner	Art Unit	
	Nicole M. Young	2139	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 October 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-38* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-38* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *10 March 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This communication is in response to the Amendment of application 10/805,702 received on October 10, 2007. Claims 1-38 are pending. Claims 1, 10, 21, and 28 are amended. Claims 35-38 are new.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1, 10, 21, and 28 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

The amended limitation reads:

> and said control verifies that said electronic device is installed in an authorized network and generates an alarm if said electronic device not present,
>
> wherein said user interface is configured to allow a user to arm and disarm a building intrusion detection features separately from security features of said LAN.

The Examiner cannot understand what is meant by "if said electronic device not present". The Examiner suggests adding a verb to the phrase between "device" and "not" to better clarify.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1 and 3-6 are rejected under 35 U.S.C. 103(a) as being anticipated by **Anderson et al. (US 2002/0091824)** herein referred to as Anderson in further view of **Alexander (US 4,647,914)** and Lau **(US 2002/0196147)**.

Claim 1 discloses an electronic device in a local area network, comprising:

a network interface that communicates with a connection point of the local area network, and that receives a polling signal from a security system in the local area network via the connection point (Figure 4 wherein the Network Switch or Hub 408 is the network interface, the Reporting and Maintenance System (RMS) 400 is the connection point and the Superintendent System 410 is the security system; Paragraph [0073] teaches the use of polling to return status information and Paragraph [0074] teaches the RMS polling); and

a control that causes the network interface to communicate a response to the security system via the connection point in response to receipt of the polling signal (Paragraph [0074] teaches the RMS sending the return messages to the superintendent system. Paragraph [0017] teaches the RMS "is provided that acts as an... Internet").

Anderson does not teach and said control verifies that said electronic device is installed in an authorized network and generates an alarm if said electronic device not present,

Lau teaches and said control verifies that said electronic device is installed in an authorized network and generates an alarm if said electronic device not present,

It would have been obvious to one of ordinary skill in the art at the time the invention was made to generate an alarm if a user when into an unauthorized area, since Lau teaches in paragraph [0046], "the invention could initiate an alarm if an inmate attempts to enter an unauthorized area or leaves an authorized area without permission. The alarm could initiate a locking command to secure exits from a vicinity. Similarly, in another embodiment, the invention could be used in a home to monitor parolees. If the parolee leaves the home or an authorized area, the system could send an alert to a monitoring computer or sound an alarm." This would ensure the user stays within the protected areas they are authorized to be in.

Anderson does not teach wherein said user interface is configured to allow a user to arm and disarm a building intrusion detection features separately from security features of said LAN.

Alexander teaches wherein said user interface is configured to allow a user to arm and disarm a building intrusion detection features separately from security features of said LAN.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to program the interface so the user can arm or disarm the detection features separate from the LAN since Alexander in column 8 under the heading "Arming Procedure-Home" that the user needs to arm the system when he or she leaves the building. This is separate from the LAN security system described above, however functions as a intrusion detection for the physical building.

Claim 3 discloses the electronic device of claim 1, wherein:

the network interface communicates, via the connection point, with a remote server that provides services for the electronic device (Paragraph 17 teaches "remotely managing multiple enterprises from a central location").

Claim 4 discloses the electronic device of claim 3, wherein:

the services include at least one of downloading software to the electronic device, performing remote programming of the electronic device, and uploading diagnostic data from the electronic device (Paragraph [0058] teaches remotely configuring door locks which is interpreted as performing remote programming. Paragraph [0073] teaches status request polling and paragraph [0074] teaches globally managed devices this is interpreted as uploading diagnostic data from the electronic device).

Claim 5 discloses the electronic device of claim 1, wherein:

the connection point comprises at least one of a hub and a gateway (Figure 4 shows the RMS comprises of both a network switch or hub and a gateway).

Claim 6 discloses the electronic device of claim 1, wherein:

the network interface receives software from the security system via the connection point for configuring the electronic device as a sensor of the security system (Paragraph [0058] teaches a temperature sensor and a door lock sensor).

Claims 21-24, 26, and 28-33 are rejected under 35 U.S.C. 103(a) as being anticipated by **Nagel et al (US 7,181,017)** in further view of **Alexander (US 4,647,914)** and Lau **(US 2002/0196147)**.

Claim 21 discloses an electronic device in a local area network, comprising:

a network interface that communicates with a connection point of the local area network; and

a control that causes the network interface to transmit a message, via the connection point, to a remote server;

wherein the message includes an address and an identifier associated with the electronic device (Figure 2 and associated text shows a user communicating through a intermediary (connection point) to a data repository (remote server) the identifier is the user private key and the address is described as either the logical address or the physical address as in column 8 lines 27-35)

Nagel does not teach and said control verifies that said electronic device is installed in an authorized network and generates an alarm if said electronic device not present.

Lau teaches and said control verifies that said electronic device is installed in an authorized network and generates an alarm if said electronic device not present,

It would have been obvious to one of ordinary skill in the art at the time the invention was made to generate an alarm if a user when into an unauthorized area, since Lau teaches in paragraph [0046], "the invention could initiate an alarm if an inmate attempts to enter an unauthorized area or leaves an authorized area without permission. The alarm could initiate a locking command to secure exits from a vicinity. Similarly, in another embodiment, the invention could be used in a home to monitor parolees. If the parolee leaves the home or an authorized area, the system could send an alert to a monitoring computer or sound an alarm." This would ensure the user stays within the protected areas they are authorized to be in.

Nagel does not teach wherein said user interface is configured to allow a user to arm and disarm a building intrusion detection features separately from security features of said LAN.

Alexander teaches teach wherein said user interface is configured to allow a user to arm and disarm a building intrusion detection features separately from security features of said LAN.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to program the interface so the user can arm or disarm the detection features separate from the LAN since Alexander in column 8 under the

heading "Arming Procedure-Home" that the user needs to arm the system when he or she leaves the building. This is separate from the LAN security system described above, however functions as a intrusion detection for the physical building.

Claim 22 discloses the electronic device of claim 21, wherein:

the remote server determines whether the address is consistent with the identifier (Figure 2 and associated text shows and teaches an authentication database in the intermediary to authenticate the user).

Claim 23 discloses the electronic device of claim 21, wherein:

the address comprises at least a portion of an Internet Protocol address (The address is described as either the logical address or the physical address as in column 8 lines 27-35, the logical address is the IP address).

Claim 24 discloses the electronic device of claim 21, wherein:

the identifier comprises a serial number (Column 16 lines the address is described as either the logical address or the physical address as in column 8 lines 27-35 teach a serial number).

Claim 26 discloses the electronic device of claim 21, wherein:

the control causes the network interface to communicate the message to the remote server as an encrypted message using an encryption code that is unique to the electronic device (in Figure 4 and associated text, column 26 lines 32-55. Nagel

teaches the user receiving the public key from the intermediary and then encrypting the plaintext message with the users unique private key and the public key).

Claim 28 discloses a security system server, comprising:

a network interface that receives a message that includes an address and an identifier associated with an electronic device;

wherein the electronic device is provided in a local area network (Figure 2 and associated text shows a user communicating through a intermediary (connection point) to a data repository (remote server) the identifier is the user private key and the address is described as either the logical address or the physical address as in column 8 lines 27-35); and

means for determining whether the address is consistent with the identifier (Figure 2 and associated text shows and teaches an authentication database in the intermediary to authenticate the user)

Nagel does not teach and said control verifies that said electronic device is installed in an authorized network and generates an alarm if said electronic device not present,

Lau teaches and said control verifies that said electronic device is installed in an authorized network and generates an alarm if said electronic device not present,

It would have been obvious to one of ordinary skill in the art at the time the invention was made to generate an alarm if a user when into an unauthorized area,

since Lau teaches in paragraph [0046], "the invention could initiate an alarm if an inmate attempts to enter an unauthorized area or leaves an authorized area without permission. The alarm could initiate a locking command to secure exits from a vicinity. Similarly, in another embodiment, the invention could be used in a home to monitor parolees. If the parolee leaves the home or an authorized area, the system could send an alert to a monitoring computer or sound an alarm." This would ensure the user stays within the protected areas they are authorized to be in.

Nagel does not teach wherein said user interface is configured to allow a user to arm and disarm a building intrusion detection features separately from security features of said LAN.

Alexander teaches teach wherein said user interface is configured to allow a user to arm and disarm a building intrusion detection features separately from security features of said LAN.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to program the interface so the user can arm or disarm the detection features separate from the LAN since Alexander in column 8 under the heading "Arming Procedure-Home" that the user needs to arm the system when he or she leaves the building. This is separate from the LAN security system described above, however functions as a intrusion detection for the physical building.

Claim 29 discloses the security system server of claim 28, wherein:

the message is received from the electronic device (Figure 2 and associated text shows a user communicating through a intermediary (connection point) to a data repository (remote server) the identifier is the user private key and the address is described as either the logical address or the physical address as in column 8 lines 27-35).

Claim 30 discloses the security system server of claim 28, wherein:

the message is received from a server that provides services for the electronic device (Figure 2 and associated text shows a user communicating through a intermediary (connection point) to a data repository (remote server) the identifier is the user private key and the address is described as either the logical address or the physical address as in column 8 lines 27-35. The server provides authentication services for the electronic device as shown).

Claim 31 discloses the security system server of claim 28, wherein:

the address comprises at least a portion of an Internet Protocol address (The address is described as either the logical address or the physical address as in column 8 lines 27-35, the logical address is the IP address).

Claim 32 discloses the security system server of claim 28, wherein:

the identifier comprises a serial number (Column 16 lines the address is described as either the logical address or the physical address as in column 8 lines 27-35 teach a serial number).

Claim 33 discloses the security system server of claim 28, wherein:

the message is received as an encrypted message using an encryption code that is unique to the electronic device (in Figure 4 and associated text, column 26 lines 32-55. Nagel teaches the user receiving the public key from the intermediary and then encrypting the plaintext message with the users unique private key and the public key).

Claims 2 and 8 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Anderson et al. (US 2002/0091824)** herein referred to as Anderson, and further in view of **Nagel et al. (US 7,181,017)** herein referred to as Nagel.

Claim 2 discloses the electronic device of claim 1, wherein:

Anderson teaches the network interface communicates with at least one other electronic device in the local area network via the connection point, Anderson does not teach but Nagel teaches to transfer entertainment content in column 15 lines 47-52. It would be obvious to someone of ordinary skill in the art at the time of invention to send entertainment content from the Internet through the intermediary. Anderson Figure 1 shows the network devices 102, 104, 06, and 108 connected through the intermediary, 110, to the Internet. The motivation to combine the entertainment content transfer as in Nagel would be in Nagel column 16 lines 63-67 and column 16 lines 1-12 where it teaches that the third party is used to cut down on network traffic, for payment options, and better encryption of the entertainment content.

Claim 8 discloses the electronic device of claim 1, wherein:

Anderson teaches claim 1. However, Anderson does not teach but Nagel teaches the control causes the network interface to communicate the response to the security system as an encrypted message using an encryption code that is unique to the electronic device in Figure 4 and associated text, column 26 lines 32-55. Nagel teaches the user receiving the public key from the intermediary and then encrypting the plaintext message with the users unique private key and the public key. It would be obvious to one of ordinary skill in the art at the time of invention to add encryption security to the communications between the security system and the end device. The motivation is stated in Nagel column 5 lines 27-37.

Claims 7, 10, and 12-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Anderson et al. (US 2002/0091824)**, and further in view of **Davies (2004/0024869), Alexander (US 4,647,914),** and Lau **(US 2002/0196147)**.

Claim 7 discloses the electronic device of claim 1, wherein:

Anderson teaches all limitations in claim 1. However, Anderson does not teach but Davies teaches the security system sets an alarm if it does not receive the response from the network interface after sending the polling signal to the network interface in paragraphs [0012] and [0013]. It would be obvious to one of ordinary skill in the art at the time of invention to set an alarm if the device does not return a response to the polling signal. The motivation is in the first few lines of Davies paragraph [0012], which teaches that the poller alerts the server if it suspects the interface is failing. In

paragraph [0010] teaches that the server sends alerts to all clients to inform them of the failed client, this would be another motivation.

Claim 10 discloses a security system, comprising:

Anderson teaches a network interface that communicates with a connection point of a local area network; and a control that causes the network interface to transmit a polling signal to an electronic device in the local area network via the connection point in Figure 4 wherein the Network Switch or Hub 408 is the network interface, the Reporting and Maintenance System (RMS) 400 is the connection point and the Superintendent System 410 is the security system; Paragraph [0073] teaches the use of polling to return status information and Paragraph [0074] teaches the RMS polling.;

Anderson does not teach but Davies teaches wherein the control sets an alarm if a response to the polling signal is not received from the electronic device in paragraphs [0012] and [0013]. It would be obvious to one of ordinary skill in the art at the time of invention to set an alarm if the device does not return a response to the polling signal. The motivation is in the first few lines of Davies paragraph [0012], which teaches that the poller alerts the server if it suspects the interface is failing. In paragraph [0010] teaches that the server sends alerts to all clients to inform them of the failed client, this would be another motivation.

Anderson does not teach and said control verifies that said electronic device is installed in an authorized network and generates an alarm if said electronic device not present,

Lau teaches and said control verifies that said electronic device is installed in an authorized network and generates an alarm if said electronic device not present,

It would have been obvious to one of ordinary skill in the art at the time the invention was made to generate an alarm if a user when into an unauthorized area, since Lau teaches in paragraph [0046], "the invention could initiate an alarm if an inmate attempts to enter an unauthorized area or leaves an authorized area without permission. The alarm could initiate a locking command to secure exits from a vicinity. Similarly, in another embodiment, the invention could be used in a home to monitor parolees. If the parolee leaves the home or an authorized area, the system could send an alert to a monitoring computer or sound an alarm." This would ensure the user stays within the protected areas they are authorized to be in.

Anderson does not teach wherein said user interface is configured to allow a user to arm and disarm a building intrusion detection features separately from security features of said LAN.

Alexander teaches teach wherein said user interface is configured to allow a user to arm and disarm a building intrusion detection features separately from security features of said LAN.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to program the interface so the user can arm or disarm the detection features separate from the LAN since Alexander in column 8 under the heading "Arming Procedure-Home" that the user needs to arm the system when he or she leaves the building. This is separate from the LAN security system described above, however functions as a intrusion detection for the physical building.

Claim 12 discloses the security system of claim 10, wherein:

the network interface communicates, via the connection point, with a remote server that provides services for the security system (Anderson paragraph 17 teaches "remotely managing multiple enterprises from a central location").

Claim 13 discloses the security system of claim 12, wherein:

when the alarm is set, the network interface communicates a message to the remote server indicating that the alarm has been set (Davies paragraph [0012], "The poller sends...one interface is failing").

Claim 14 discloses the security system of claim 13, wherein:

the message comprises an identifier of the electronic device (Davies paragraphs [0012], when the poller sends the notification of the interface failing it sends an id of the failing device).

Claim 15 discloses the security system of claim 13, wherein:

the message comprises at least a portion of an Internet Protocol address associated with the electronic device (Davies paragraph 37 teaches that the message

comprises of at least the Internet Protocol address. Paragraph [0042] shows the message format which includes "IP Address").

Claim 16 discloses the security system of claim 10, wherein:

the connection point comprises at least one of a hub and a gateway (Anderson Figure 4 shows the RMS comprises of both a network switch or hub and a gateway).

Claim 17 discloses the security system of claim 10, wherein:

the network interface transmits software to the electronic device via the connection point to configure the electronic device as a sensor of the security system (Anderson paragraph [0058] teaches a temperature sensor and a door lock sensor).

Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over **Anderson et al. (US 2002/0091824)**, and further in view of **Harkins (US 6,038,322)**.

Claim 9 discloses the electronic device of claim 1, wherein:

Anderson teaches claim 1. However, Anderson does not teach, but Harkins teaches the control causes the network interface to communicate the response to the security system as an encrypted message using an encryption code that is unique for a specified group of electronic devices in column 2 lines 16-41 wherein group members share a group encryption key. It would be obvious to one of ordinary skill in the art at the time of invention to add group encryption to a message. The motivation would be in Harkins column 1 lines 10-15 where it states cryptography is used to secure messages traveling over public transportation. Harkins column 1 lines 25-36 teach an advantage to using group common secret keys.

Claims 11 and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Anderson et al. (US 2002/0091824)**, and of **Davies (2004/0024869)** as applied above, and further in view of **Nagel et al. (US 7,181,017)** herein referred to as Nagel.

Claim 11 discloses the security system of claim 10, wherein:

Anderson and Davies teach the limitations of claim 10 as above. They do not teach but Nagal teaches, the electronic device communicates with at least one other electronic device in the local area network via the connection point to transfer entertainment content in column 15 lines 47-52. It would be obvious to someone of ordinary skill in the art at the time of invention to send entertainment content from the Internet through the intermediary. Anderson Figure 1 shows the network devices 102, 104, 06, and 108 connected through the intermediary, 110, to the Internet. The motivation to combine Anderson and Davies with the entertainment content transfer as in Nagel would be in Nagel column 16 lines 63-67 and column 16 lines 1-12 where it teaches that the third party is used to cut down on network traffic, for payment options, and better encryption of the entertainment content.

Claim 19 discloses the security system of claim 10, wherein:

Anderson and Davies teach the limitations of claim 10 above. However, Anderson and Davies do not teach, but Nagel teaches the response to the polling signal is provided as an encrypted message using an encryption code that is unique to the electronic device in Figure 4 and associated text, column 26 lines 32-55. Nagel teaches the user receiving the public key from the intermediary and then encrypting the plaintext message with the users unique private key and the public key. It would be obvious to

one of ordinary skill in the art at the time of invention to add encryption security to the communications between the security system and the end device in Anderson and Davies. The motivation is stated in Nagel column 5 lines 27-37.

Claim 18 is rejected under 35 U.S.C. 103(a) as being unpatentable over **Anderson et al. (US 2002/0091824)**, and of **Davies (2004/0024869)** as applied above, and further in view of **Stilp (US 2004/0212493).**

Claim 18 discloses the security system of claim 10, further comprising:

Anderson and Davies do not teach but Stilp teaches a means for monitoring at least one sensor for detecting intrusion in a building in paragraph [0019]. Stilp teaches RFID readers and RFID transponders that are "capable of causing an alert in the event of intrusion" in a building. The RFID is interpreted by the Examiner to be the sensor and the RFID transponder is interpreted to be the means for monitoring the sensor. It would be obvious to one of ordinary skill in the art at the time of invention to use the system of Anderson with the alarm of Davies to monitor intrusion into the building as in Stilp. The motivation for combining Anderson and Davies is the same as above. The motivation for combining Anderson and Davies with Stilp is that Anderson paragraph [0058] teaches a temperature sensor and a door lock sensor and electronic locks on the door. It would be obvious to then use the door lock sensor as the sensor in Stilp is used to alert if there is an intrusion in the building.

Claim 20 is rejected under 35 U.S.C. 103(a) as being unpatentable over **Anderson et al. (US 2002/0091824)**, and of **Davies (2004/0024869)** as applied above, and further in view of **Harkins (US 6,038,322).**

Claim 20 discloses the security system of claim 10, wherein:

Anderson and Davies teach the limitations of claim 10 as above. Anderson and Davies do not teach, but Harkins teaches the response to the polling signal is provided as an encrypted message using an encryption code that is unique for a specified group of electronic devices in column 2 lines 16-41 wherein group members share a group encryption key. It would be obvious to one of ordinary skill in the art at the time of invention to add group encryption to a message. The motivation would be in Harkins column 1 lines 10-15 where it states cryptography is used to secure messages traveling over public transportation as are the messages in Anderson and Davies. Harkins column 1 lines 25-36 teach an advantage to using group common secret keys.

Claim 25 is rejected under 35 U.S.C. 103(a) as being unpatentable over **Nagel et al (US 7,181,017)**, as applied above, and further in view of **Stilp (US 2004/0212493).**

Claim 25 discloses the electronic device of claim 21, wherein:

the message is transmitted to the remote server using cryptographic data and an authentication protocol that are also used by a security system that communicates with the remote server via the connection point to report an intrusion in a building Stilp teaches a means for monitoring at least one sensor for detecting intrusion in a building in paragraph [0019]. Stilp teaches RFID readers and RFID transponders that are

"capable of causing an alert in the event of intrusion" in a building. The RFID is interpreted by the Examiner to be the sensor and the RFID transponder is interpreted to be the means for monitoring the sensor. It would be obvious to one of ordinary skill in the art at the time of invention to use the system of Nagel to monitor intrusion into the building as in Stilp. The motivation for combining Nagel with Stilp is that Anderson paragraph [0058] teaches a temperature sensor and a door lock sensor and electronic locks on the door. It would be obvious to then use the door lock sensor as the sensor in Stilp is used to alert if there is an intrusion in the building. The alarm system is taught in Stilp paragraph [0021].

Claims 27 and 34 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Nagel et al (US 7,181,017)** as applied above, and further in view of **Harkins (US 6,038,322)**.

Claim 27 discloses the electronic device of claim 21, wherein:

Nagel teaches the limitations in claim 21 above. Nagel does not teach, but Harkins teaches the control causes the network interface to communicate the message to the remote server as an encrypted message using an encryption code that is unique for a specified group of electronic devices. Harkins teaches the control causes the network interface to communicate the response to the security system as an encrypted message using an encryption code that is unique for a specified group of electronic devices in column 2 lines 16-41 wherein group members share a group encryption key. It would be obvious to one of ordinary skill in the art at the time of invention to add group

encryption to a message. The motivation would be in Harkins column 1 lines 10-15 where it states cryptography is used to secure messages traveling over public transportation as are the messages in Nagel. Harkins column 1 lines 25-36 teach an advantage to using group common secret keys.

Claim 34 discloses the security system server of claim 28, wherein:

Nagel teaches the limitations of claim 28 as above. Nagel does not teach, but Harkins teaches the message is received as an encrypted message using an encryption code that is unique for a specified group of electronic devices. Harkins teaches the control causes the network interface to communicate the response to the security system as an encrypted message using an encryption code that is unique for a specified group of electronic devices in column 2 lines 16-41 wherein group members share a group encryption key. It would be obvious to one of ordinary skill in the art at the time of invention to add group encryption to a message. The motivation would be in Harkins column 1 lines 10-15 where it states cryptography is used to secure messages traveling over public transportation as are the messages in Nagel. Harkins column 1 lines 25-36 teach an advantage to using group common secret keys.

Regarding **(new) claims 35-38** wherein said control of claims 1, 10, 21, and 28 respectively is configured to not allow spoofing of said electronic device. **Anderson et al. (US 2002/0091824**) teaches this limitation in paragraph [0008]. Each device is given a unique idea to use for authorization.

Note: Examiner has pointed out particular references contained in the prior arts of record and in the body of this action for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. Applicant should consider the entire prior art as applicable to the limitations of the claims. It is respectfully requested from the applicant, in preparing for response, to consider fully the entire reference as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior arts or disclosed by the Examiner.

Response to Arguments

Applicant's arguments with respect to claims 1, 10, 21, and 28 have been considered but are moot in view of the new ground(s) of rejection.

New art, **Alexander (US 4,647,914)** and Lau **(US 2002/0196147)**, has been brought in to reject the additional limitations added to claims 1, 10, 21 and 28.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP

§ 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nicole M. Young whose telephone number is 571-270-1382. The examiner can normally be reached on Monday through Friday, alt Fri off, 8:00am-5:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

NMY
12/13/2007

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100